Looking at Construction of $\mathbb{Z}/m\mathbb{Z}$ again

Summary: We defined an equivalence relation on $\mathbb{Z}$ & $\mathbb{Z}/m\mathbb{Z}$ is just a set of those equivalence classes.

Goal: Let us try to generalize this Construction in terms of subgroups.

$(\mathbb{Z}, +)$ is a group.

Qn: What are all the subgroups of $(\mathbb{Z}, +)$?

Ans: $\{0\}$, $\mathbb{Z}$ are obvious ones.

Suppose H is a subgroup of $\mathbb{Z}$ that is not $\{0\}$ or $\mathbb{Z}$.

Here are some observations about H

i) $1 \notin H$ because then $H = \mathbb{Z}$.

ii) H contains both positive and negative integers.

Suppose m is the smallest positive integer that lies in H.

Then $H = \{\ldots, -2m, -m, 0, m, 2m, 3m, \ldots\}$

because if $b > 0 \in H$ & b is not a multiple of m then

$$b = mq + r \quad 0 < r < m$$

$$r = \underbrace{b - mq}_{\in H}$$

which is contradiction

Let's denote $H = \{\ldots, -m, 0, m, 2m, \ldots\}$ as $m\mathbb{Z}$.

So, all the subgroups of $\mathbb{Z}$ are of the form $m\mathbb{Z}$.

Equivalence Relation	Restating that in terms of subgroups
$a \sim b \iff a$ & b leave the same remainder when divided by m $\iff a-b$ is a multiple of m	$a \sim b \iff a-b \in m\mathbb{Z}$ in general G group H subgroup of G $a \sim b \iff ab^{-1} \in H$

Let's explore this!

G group $\quad H \leq G$ Subgroup

Define a relation on G as follows:

$$a \sim b \iff ab^{-1} \in H$$

Equivalence classes are called <u>Cosets</u>.

$$G/H = \{ \text{Set of cosets} \}$$

$ab^{-1} \in H$, $ab^{-1} = h$ for some $h \in H$

$$a = hb$$

$$a \in Hb$$

$$G/H = \{ Hb \mid b \in G \}$$

Some questions to ponder:

1. Is G/H a group?
2. Is G/H always finite?

$G/H = \{ Hb \mid b \in G \}$

A natural way to multiply two cosets is as follows:

$$Hb_1 \, Hb_2 = H\, b_1 b_2$$

but this has some issues!

An element in $Hb_1\, Hb_2$ looks like

$h_1 b_1 \, h_2 b_2$ — this is not necessarily of the form $h_3 b_1 b_2$

But now, suppose $gHg^{-1} = H$ for all $g \in G$,

$$\| $$

$$\{ ghg^{-1} \mid h \in H \}$$

Then $h_1 b_1 \, h_2 b_2 = h_1 (b_1 h_2) b_2$

$= h_1 (h' b_1) b_2$

So, $Hb_1 \, Hb_2 = H\, b_1 b_2$

Defn: Let G be a group. Suppose H is a subgroup of G. We say that H is <u>normal</u> in G if $gHg^{-1} = H$ for all $g \in G$.

Thm: Let H be a normal subgroup of G. Then $G/H = \{ Hb \mid b \in G \}$ is a group.

Pf: 1) $(Hb_1)(Hb_2) = Hb_1b_2$

2) Associativity

$$(Hb_1)(Hb_2 Hb_3) = Hb_1 Hb_2 b_3 = H b_1 b_2 b_3$$

$$(Hb_1 Hb_2)(Hb_3) = (H b_1 b_2) Hb_3 = H b_1 b_2 b_3$$

3) Identity coset is He (e is identity of group)

$$(Hb)(He) = H(be) = Hb$$

$$(He)(Hb) = H(eb) = Hb$$

4) Inverse

$Hb^{-1}\ Hb = Hb^{-1}b = He$

$Hb\ Hb^{-1} = Hbb^{-1} = He$

Corollary: Let G be an abelian group. Let H be a subgroup of G. Then G/H is a group.

Pf: Since G is abelian, H is already normal, because

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$
$$= \{hgg^{-1} \mid h \in H\}$$
$$= \{h \mid h \in H\}$$
$$= H$$

So G/H is a group.

Defn: G/H is called quotient group of G by H.

Examples:

1) $G = S_3 = \{e, (12), (13), (23), (123), (132)\}$

Subgroups of G are

$\{e\}, G, \{e, (12)\}, \{e, (13)\}, \{e, (23)\}, \{e, (123), (132)\}$

Among these normal subgroups are

$\{e\}, G, \{e, (123), (132)\}$

$= A_3$

$G/\{e\} = G$

$G/G = \{e\}$

$G/A_3 = \{e, \overline{(12)}\}$

2) $G = \mathbb{Z}$

$H = m\mathbb{Z}$

$$G/H = \mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \ldots, m-1\}$$

Group homomorphisms give us a source of normal subgroups.

$$\varphi : G_1 \longrightarrow G_2$$

↙ group homomorphism

Lemma: $\ker\varphi$ is a normal subgroup of G_1.

Pf: We want to show that

$$g \ker\varphi\, g^{-1} = \ker\varphi \quad \forall g \in G.$$

We will first show that $g \ker\varphi\, g^{-1} \subseteq \ker\varphi$

If $gxg^{-1} \in g \ker\varphi g^{-1}$, then

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1})$$
$$= \varphi(g)\varphi(g^{-1}) = e$$

We will now show that $\ker\varphi \subseteq g \ker\varphi g^{-1}$

if $x \in \ker\varphi$

$$x = g(g^{-1}xg)g^{-1}$$

$$\uparrow$$

$$\ker\varphi$$

$$\Rightarrow x \in g \ker\varphi g^{-1}.$$

So, $\ker\varphi = g\ker\varphi g^{-1} \quad \forall\, g \in G.$

More examples

1) $\varepsilon : S_n \to \{\pm 1\}$

↳ signature

$\ker(\varepsilon) = A_n$

$A_n \trianglelefteq S_n$

2) $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$

$\ker(\det) = SL_n(\mathbb{R})$

$SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$

3) $\varphi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

$x \longmapsto x \pmod m$

$\ker \varphi_m = \{ x \mid x \pmod m = 0 \}$

$= \{ x \mid x \text{ is a multiple of } m \}$

$= m\mathbb{Z}$

FIRST ISOMORPHISM THEOREM

Thm: $\varphi : G_1 \to G_2$

└ group isomorphism

Then $G_1/\ker\varphi \cong \text{im}\,\varphi$, i.e.

$G_1/\ker\varphi$ are isomorphic as groups.

Pf: We will construct a map f from

$$G_1/\ker\varphi \longrightarrow \operatorname{im}\varphi$$

and show that it is an isomorphism.

$$G_1/\ker\varphi = \{(\ker\varphi)g \mid g \in G_1\}$$

Define $f((\ker\varphi)g) = \varphi(g)$

1) Need to check f is well-defined ie

if $(\ker\varphi)g_1 = (\ker\varphi)g_2$ then

$f((\ker\varphi)g_1) = f((\ker\varphi)g_2)$

Pf $(\ker\varphi)g_1 = (\ker\varphi)g_2$

$\Rightarrow g_1 g_2^{-1} \in \ker\varphi$

$\Rightarrow \varphi(g_1 g_2^{-1}) = e$

$\Rightarrow \varphi(g_1) = \varphi(g_2)$

2) f is a group homomorphism.

$$f\left((\ker\varphi)\, g_1 \cdot (\ker\varphi)\, g_2\right)$$

$$= f\left((\ker\varphi)\, g_1 g_2\right)$$

$$= \varphi(g_1 g_2)$$

$$= \varphi(g_1)\ \varphi(g_2)$$

$$= f\left((\ker\varphi)\, g_1\right)\ f\left((\ker\varphi)\, g_2\right)$$

3) $\ker f = \{(\ker\varphi) g \mid \varphi(g) = e\}$

$$= \{(\ker\varphi)\, e\}$$

$\Rightarrow f$ is injective

4) f is surjective

Pick $x \in \operatorname{im}\varphi$

$$x = \varphi(g) = f\left((\ker\varphi) g\right)$$

Examples:

1) G group, e is identity of G

$$\varphi : G \longrightarrow \{e\}$$

$$g \longmapsto e$$

$$\ker \varphi = G$$

$$G/G \cong \{e\}$$

2) $$\varepsilon : S_n \longrightarrow \{\pm 1\}$$

$$\sigma \longmapsto \text{signature}(\sigma)$$

$$\ker \varepsilon = A_n$$

$$S_n/A_n = \{\pm 1\}$$

3) $$\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$$

$$A \longmapsto \det(A)$$

$$\ker(\det) = SL_n(\mathbb{R})$$

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$$